REMARKS

Claims 1-15 remain in the application. In the Office Action dated November 18, 2004, claims 2-4, 7-9, and 13-15 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Claims 1, 5, 6, and 10-12 were rejected under 35 U.S.C. 103(a) as being unpatentable over reference titled "Copy Protection for SRAM based FPGA Designs", by David Kessner (hereinafter referred as Kessner), in view of PCT publication WO99/30499 invented by Eskicioglu (hereinafter referred as Eskicioglu). The applicant respectfully disagrees with the Examiner's conclusion.

Claim Rejections-35 U.S.C. 112

Claims 2-4, 7-9, and 13-15 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. More particularly, the Examiner stated that claims 2, 7, and 13 recite that two encryptions are performed before the decryption, and claims 3, 10, and 14 make clear that it is only one decryption takes place after the two encryptions, however encryption algorithms generally require one decryption operation to correspond to one encryption operation. The applicant respectfully disagrees with the Examiner's conclusion.

It is not necessary that one decryption operation corresponds to one encryption operation. For example, if a first encryption key is k_0 and a second encryption key is k_1, a decryption key corresponding to the encryptions k_0 and k_1 is not necessary to be the direct reverse operations of k_0 or k_1. The decryption key can be an operation that reverses the total encryption effect of the two encryption keys k_0 and k_1. The result of decryption will be the original code before encryption. Therefore, the application complies with the enablement requirement of 35 U.S.C. 112 and the rejections to claims 2-4, 7-9, and 13-15 should be reconsidered and withdrawn.

Claim Rejections -35 U.S.C. 103

Claims 1, 5, 6, and 10-12 were rejected under 35 U.S.C. 103(a) as being unpatentable over reference titled "Copy Protection for SRAM based FPGA Designs", by David Kessner, in view of PCT publication WO99/30499 invented by Eskicioglu. Issue is taken with that position.

Kessner discloses a design of an FPGA device with a copy protection mechanism. The design in Kessner includes a CPLD and an FPGA, each of which includes a Linear Feedback

Shift Register (LFSR). The two LFSR's are identical. The two identical LFSR's are initialized by a "key"to generate outputs, which are compared in the FPLA. If the outputs are identical, the operation of the FPGA is allowed.

Eskicioglu teaches a method of protecting audio/video data in its transmission line from illegally interception and copying. Typically, audio/video data is encrypted at the transmitter before it is broadcast. The receiver includes a host device (e.g., digital television receiver, video cassette recorder) and a smart card, which decrypts the encrypted data. When the decrypted signal is transmitted from the smart card to the host device, the security maybe breached and the decrypted data maybe captured. The disclosure of Eskicioglu is directed to secure the transmission between the smart card and the host device. In order to do so, the host device sends a seed to the smart card, which re-encrypts the data using an encryption key corresponding to the seed, and then sends the re-encrypted data to the host device. Even the signal is captured in transmission between the smart card and the host device, because it is re-encrypted, the data cannot be accessed.

As discussed above, Kessner discloses the use of a CPLD in an FPGA device to prevent from copying the FPGA device by reverse engineering. Eskicioglu is directed to secure data transmission to prevent from interception of the data transmitted. These two prior art references are in different technology fields and neither of the references suggests to combine them together. The present invention includes a CPLD and an FPGA, and further includes encryption and decryption devices to secure the data transmission between the CPLD and the FPGA. The conventional encryption and decryption techniques have been in the art for a long time, but no prior art recognizes the need of encryption of data in an FPGA device or incorporates these encryption and decryption techniques in CPLD and FPGA devices. Therefore, the applicant respectfully submit that the Examiner's conclusion that combining the FPGA design in Kessner and the encryption technique in Eskicioglu would render the present invention obvious is based on hindsight.

Furthermore, in contrast to the two prior art references, in the present application, claim 1 claims a copy protection system for FPGA. The copy protection system uses a CPLD to generate an initial state to initialize a first sequence generator in the CPLD and a second sequence generator in the FPGA. The FPGA includes a third sequence generator to generate a challenge sequence, which is sent to the initialized first and second sequence generator. If the

outputs from the first and second sequence generators corresponding to the challenge sequence are the same, the operation of the FPGA is allowed.

In Kessner, the LFSR's are initialized with a "key". Kessner fails to teach how to generate the "key". Moreover, the present application not only requires a key to initialize the first and second sequence generators, but also requires a challenge sequence to further test the authenticity of the devices. In contrast, in Kessener, after the LFSR's in the CPLD and the FPGA are initialized, the outputs of the LFSR's are compared. Kessener lacks the configuration for generating a challenge sequence and further testing the authenticity of the devices.

Eskicioglu teaches a method of encrypting data for protecting data when they are transmitted. The Examiner stated that Eskicioglu teaches the use of a challenge sequence at pages 7 and 8. However, pages 7 and 8 of Eskicioglu teach a method of generating a shared key by the host and the smart card, so that the data transmitted between the host and the smart card can be encrypted and decrypted by using the shared key. Eskicioglu does not teach a third sequence generator for sending a challenge sequence to both devices and a comparator for comparing the responses from both devices to authenticate the two devices. Therefore, Eskicioglu does not teach or suggest the present invention.

Therefore, for the foregoing reasons, claim 1 requires the use of a first "key" from the CPLD to initialize the first and second sequence generators, and a second "key" from the FPGA to further test the authenticity of the CPLD and the FPGA. Neither Kessner nor Eskicioglu teaches the two-step authentication mechanism as claimed in claim 1. The combination of Kessner and Eskicioglu also does not teach or suggest the present invention. Therefore, the present invention as claimed in claim 1 is not obvious over Kessner in view of Eskicioglu.

Claims 2-4 depend from claim 1 and include all the limitations of claim 1. Therefore, claims 2-4 should be considered patentable.

Claim 5 is an independent claim, which claims a copy protection system including a CPLD and an FPGA. The system further includes encryption and decryption devices. As discussed above, no prior art reference recognizes the need of encryption of the data transmitted between the CPLD and the FPGA. The cited prior art references Kessner and Eskicioglu are in different technology fields and there is no suggestion to combine them together. Therefore, the applicant respectfully submits that claim 5 should be considered patentable over Kessner and Eskicioglu. Dependent claims 6-8 depend from claim 5 and also should be considered

patentable.

Claim 10 is an independent claim. For the same reason as in the argument regarding claim 5, no prior art reference teaches or suggests the use of encryption and decryption in an FPGA device. Therefore, claim 10 should be considered patentable over the cited references. Claims 11-15 depend from claim 10 and also should be considered patentable over the cited references.

Conclusion

The applicant, accordingly, respectfully submits that in view of the preceding arguments, claims 1-15 are patentable over the cited references, whether considered alone or in combination, and respectfully request reconsideration and withdrawal of the rejections of these claims under 35 U.S.C. 103(a). If a telephone conference will expedite prosecution of the application the Examiner is invited to telephone the undersigned.

No additional costs are believed to be due in connection with the filing of this paper. However, the Commissioner is hereby authorized to charge any additional fees, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

McDermott Will & Emery LLP

Date: 4 JAN 2005

Mark G. Lappin, P.C., Reg. No. 26,618
Attorneys for Applicants
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800